

Pg 1 of 18, ATTACKERS EXHIBIT FACEBOOK GOOGLE- 5.23.22 – NorCal 9th District -

CASE NO.: 22-cv-1107-TSH

Name: SD Redmond
Address: 210 S. Ellsworth Ave, #1275
San Mateo, CA 94401
Phone Number: 510-868-2862
E-mail Address: justice@majestic111.com

EVIDENCE/EXHIBIT COPIES AT:

<https://www.majestic111.com>
<http://www.the-truth-about-the-dept-of-energy.com>
<https://san-francisco-news.com>

PLAINTIFF, A Pro Se, disabled, non-lawyer, federal witness who has requested Court appointed counsel

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

(UNLIMITED CIVIL JURISDICTION)

**SD REDMOND, a Pro Se non-lawyer federal
whistle-blower/witness**

PLAINTIFF,

v.

UNITED STATES OF AMERICA

DEFENDANTS.

) **CASE NO.: 22-cv-1107-TSH**
)
) **ATTACKERS EXHIBIT**
) **FACEBOOK/GOOGLE 5.23.22**
)
) **INTENTIONAL FRAUD; CONCEALMENT**
) **FRAUD; NEGLIGENT**
) **MISREPRESENTATION; INTENTIONAL**
) **INFLICTION OF EMOTIONAL DISTRESS;**
) **RICO RACKETEERING;**
) **ANTI-TRUST/MONOPOLY; COURT**
) **ORDER DEMANDED FOR FULL SSDI**
) **BACK PAYMENTS; AND SUCH OTHER**
) **CLAIMS LISTED HEREIN UNDER**
) **“CLAIMS” SECTION**

Filed: May 23, 2022

DEMAND FOR JURY TRIAL

**ADDITIONAL EXHIBITS TO BE FILED
ELECTRONICALLY AND NOW
AVAILABLE, ON THE WEB, TO THE
PUBLIC, GLOBALLY, AT LINKS
ABOVE AND MIRROR SITES**

ATTACKERS EXHIBIT FACEBOOK/GOOGLE 5.23.22

1
2 United States Government executives including Dianne Feinstein, and her family; Nancy
3 Pelosi, and her family; Kamala Harris and her family; Jennifer Granholm, and her family, Barack
4 Obama, and his family; and current and past White House officials, and their families, own
5 Facebook, Google, Netflix and their affiliates. They have hired their staffing from those companies
6 taken orders from those companies, commanded those companies to harm their enemies and
7 whistle-blowers, received BILLIONS of dollars of unreported political campaign financing from
8 those companies via indirect cash and internet manipulation services. These, and other government
9 officials ordered Facebook, Google, Netflix to harm Plaintiff because he was a whistle-blower and
10 a competitor. In fact, in a recent federal hearing at the United States Patent Office, the USPTO
11 determined that Plaintiff had invented the core technology that Facebook relies on, but government
12 officials blockaded Plaintiff's issuance of the paperwork to monetize that fact because Facebook
13 and Google's skills work in, and operate control over, the USPTO. In another case, government
14 officials ordered Facebook and it's "Cartel"; and Google and it's "Cartel" to blockade all media
15 coverage of Plaintiff's electric car company while exclusively promoting Tesla's car company,
16 which government officials own covert stock in. Defendants have made comments to the Court and
17 officials that they plan to use a strategy of further defamation against Plaintiff by trying to label him
18 as a "crazy inventor" and that Defendants will seek to portray their ownerships and control of
19 Facebook and Google, in particular, as "benign" support for a "benign entity" which Plaintiff is
20 making "wild conspiracy assertions" about. A long time favored tactic of Defendant.

21
22 Alas, though: An assertion is not a "Conspiracy Theory" when the assertion is based on
23 FACTS!

24
25 Recently the District of Columbia (the "District"), by the Office of the Attorney General,
26 brought an action against Defendant Mark Zuckerberg, who Plaintiff was up against in his recent
27
28

CASE NO.: 22-cv-1107-TSH

USPTO hearing, for violations of the District’s Consumer Protection Procedures Act, D.C. Code §§ 28-3901, *et seq.* (“CPPA”). In support of its claims, the District stated as follows:

“In addition to the following allegations, this District is also in possession of significant evidence that further demonstrates both the propriety of the Court’s exercise of personal jurisdiction over Mr. Zuckerberg as well as his violations of the CPPA. That evidence was obtained through discovery in the District’s litigation against Facebook (now Meta Platforms, Inc.). District of Columbia v. Facebook, Inc. , 2018 CA 008715 B. In an excess of caution regarding the protective order issued in that action, the District has served discovery requests with this complaint for re-production of that material in this case, among other requests. See D.C. Super. Ct. R. 26 cmt. (a) (1) (“The Superior Court rules allow parties to begin discovery at the filing of the complaint; this process gives parties greater options for early discovery than those available under the Federal Rules.”). Citations to that additional evidence do not presently appear in this complaint, and the District will amend (either by right or with leave of Court) once it has obtained that information from Defendant or Facebook directly. “

Introduction

1. In under two decades, Facebook, Inc. (now known as Meta Platforms, Inc.) (“Facebook”) has grown from a small online social network to an implacable corporate giant.

Facebook offers a variety of products and services, including the well-known Facebook product.

Today, Facebook is larger than any single country—with more than 2.9 billion monthly active users, nearly half the global population. To put that in perspective, Facebook has more users than the populations of the United States, China and Brazil combined. And Facebook has become wealthier than over 150 countries worldwide, including Switzerland, Sweden, and the UAE. Not surprisingly, Facebook has seized enormous influence over global affairs. Facebook controls how

CASE NO.: 22-cv-1107-TSH

1 people communicate with friends and family, conduct business online, what news they read, and
2 even how they communicate with governments and elected officials. Atop it all is Mark
3 Zuckerberg, the unelected leader of a massive digital empire with billions of inhabitants.

4 2. But Zuckerberg’s Facebook is far from a disinterested platform for people to communicate, stay
5 in touch with friends, and reconnect with old acquaintances. Instead, Facebook has become a wildly
6 successful and unique business, deriving enormous wealth from acquiring and monetizing the data
7 of those billions of people leading their lives in Facebook’s digital ecosystem. But even that is not
8 enough. Facebook is in a relentless pursuit to expand its reach on humanity and bring an ever-
9 increasing number of people under its influence.
10

11 3. To that end, Mark Zuckerberg has been building his version of the Internet where the “default is
12 social.” To him, that means building an Internet where people live their digital lives on Facebook.
13 The goal is to convince people to reveal the most granular details of who they are to Facebook—
14 their religions, their work histories, their likes—so that it can be monetized, and Zuckerberg and his
15 company can continue to grow even wealthier.
16

17 4. Facebook—at Zuckerberg’s direction—shifted its business model in this way because it
18 recognized that it could be even more profitable if it could harness and sell the ability to dependably
19 influence its users’ behavior to third parties. Facebook therefore encouraged (and, at times, teamed
20 up with) developers and researchers to collect and analyze Facebook user data so that it could better
21 learn how to manipulate its own users’ moods and influence what they purchase and even whether
22 and how they vote.
23

24 5. Facebook has become among the world’s leading innovators in experimenting on how to keep
25 users engaged—meaning more data and more money for Facebook. But at Facebook’s scale, these
26 experimental decisions reverberate globally.
27
28

CASE NO.: 22-cv-1107-TSH

1 6. That is in part because Facebook has realized an ugly truth: its social platform becomes
2 “stickier” (meaning people will stay on it longer and share more data) when it is filled with toxicity.
3 What this means is that the more Zuckerberg’s Facebook stokes divisiveness and polarization,
4 destabilizes democracies, amplifies genocides, and impacts users’ mental health, the more money
5 Facebook and its leaders make.

6 7. Given the trillions of dollars at issue, and having no regard for the people it purports to serve,
7 Facebook—at Zuckerberg’s direction—has decided to hide these problems for as long as possible,
8 including intentionally misleading Facebook users as well as the public, the press, and political
9 leaders.
10

11 8. One prime example—and the one that forms the basis for the instant suit—was Facebook’s 2010
12 decision to open up the Facebook Platform to third parties. Again the brainchild of Zuckerberg, this
13 move helped Facebook by persuading outside developers to build eye-catching applications for
14 Facebook—directing even more users, and user data, into the platform. Developers, though, could
15 access the massive trove of user data that Facebook had collected through the “side door” of
16 applications.
17

18 9. Zuckerberg had always been aware that the success of Facebook hinged on convincing users that
19 their data was private enough, while selling as much access to those users as possible without
20 driving them away. And Zuckerberg was fully aware that users would be concerned by this newly
21 vulnerable position. So Zuckerberg engaged in a decade-long campaign designed to convince users
22 that Facebook cared about and tried to protect users and their data. Behind closed doors however,
23 Zuckerberg insisted that Facebook’s policies be “as simple as we can get away with.”² Given that
24 Facebook’s platform was designed to allow abuse, Zuckerberg’s company largely operated without
25 proper safeguards in place to protect users: policy enforcement was lax, review of app violations
26
27
28

CASE NO.: 22-cv-1107-TSH

1 was inconsistent or subjective, and the policies themselves were unclear and confusing. But in 2018,
2 the world learned of this sham.

3 10. In March 2018, whistleblower Christopher Wylie publicly revealed that a company called
4 Cambridge Analytica—a London-based electioneering firm—exfiltrated the personal data of more
5 than 70 million Facebook users in the United States, including more than 340,000 District residents,
6 in order to influence the results of the 2016 United States presidential election. This data trove
7 included Facebook users' ages, interests, pages they've liked, groups they belong to, physical
8 locations, political affiliation, religious affiliation, relationships, and photos, as well as their full
9 names, phone numbers, and email addresses.
10

11 11. In other words, Cambridge Analytica used the Facebook Platform—in a way that Facebook and
12 Zuckerberg encouraged—to influence and manipulate the outcome of a United 2
13 Email from Mark Zuckerberg to Sam Lessin (Nov. 19, 2012, 10:39 a.m.), available at
14 [https://dataviz.nbcnews.com/projects/20191104-facebook-leaked-documents/assets/facebook-](https://dataviz.nbcnews.com/projects/20191104-facebook-leaked-documents/assets/facebook-sealed-exhibits.pdf)
15 [sealed-exhibits.pdf](https://dataviz.nbcnews.com/projects/20191104-facebook-leaked-documents/assets/facebook-sealed-exhibits.pdf).
16

17 States presidential election. The personal data of the more than 70 million U.S. Facebook users that
18 Cambridge Analytica used to manipulate the election accounted for more than half the total votes
19 during the 2016 presidential elections, in an election that was effectively decided by just a few
20 hundred thousand people.

21 12. Though the data Cambridge Analytica (and many other companies like Media Matters, Fusion
22 GPS, Black Cube and other attack services) used was supposedly private and protected from
23 disclosure by Facebook's privacy and data policies, Cambridge Analytica knew that it could access
24 this trove of data using Facebook's existing developer tools, an open secret that was well known to
25 Facebook's business partners using the platform. Cambridge Analytica also knew that it could
26 leverage Facebook's lax policy enforcement to continue manipulating the Facebook data it had
27
28

CASE NO.: 22-cv-1107-TSH

1 amassed without fear Facebook would do anything about its operations. All the while, Facebook
2 and Zuckerberg were trying to convince users in their user-facing statements that their data was
3 safe.

4 13. The Cambridge Analytica revelations shocked the world, but it was no surprise to Facebook or
5 Zuckerberg. Facebook had both a longstanding relationship with Cambridge Analytica and also
6 actively encouraged companies like Cambridge Analytica to use the Facebook Platform to influence
7 and manipulate consumer behavior.

8
9 14. What is most troubling is that Facebook looked into Cambridge Analytica and determined that
10 it posed a risk to consumer data but chose to bury those concerns rather than stop them, as that
11 could have hurt Facebook's (and Zuckerberg's) bottom line. Instead of coming clean, Facebook
12 continued to help Cambridge Analytica win a United States presidential election.

13 15. While Facebook and Zuckerberg have, a full three years later, publicly condemned Cambridge
14 Analytica's data collection, its condemnation, in reality, only demonstrates that what Zuckerberg
15 and Facebook say publicly is part of an intentional plan to mask the devastating consequences of
16 their actions (or inactions).

17
18 16. Zuckerberg has said time and again that he and Facebook have a responsibility to protect users,
19 and if they can't, then they "don't deserve to serve [them]."

20 17. Accordingly, the District brings this case to ensure that Mark Zuckerberg is held accountable
21 for his role in Facebook violating the District's consumer protection laws by misrepresenting the
22 protection of user data and their blatant disregard and misuse of sensitive, personal data belonging
23 to District residents.

24
25 The District of Columbia is a municipal corporation empowered to sue and be sued and is the local
26 government for the territory constituting the permanent seat of the federal government. The District
27 brings this case through the Attorney General for the District of Columbia, who is the chief legal
28

CASE NO.: 22-cv-1107-TSH

1 officer for the District. The Attorney General is responsible for upholding the public interest and is
2 also specifically authorized to enforce the District’s consumer protection laws, including the CPPA.

3
4 Mark Zuckerberg, FACEBOOK (Mar. 21, 2018), [https://www.facebook.com/zuck/posts/i-want-to-](https://www.facebook.com/zuck/posts/i-want-to-share-an-update-on-the-cambridge-analytica-situation-including-the-ste/10104712037900071/)
5 [share-an-update-on-the-cambridge-analytica-situation-including-the-ste/10104712037900071/](https://www.facebook.com/zuck/posts/i-want-to-share-an-update-on-the-cambridge-analytica-situation-including-the-ste/10104712037900071/) (last
6 visited May 20, 2022)

7 Defendant Mark Zuckerberg is an individual residing in Palo Alto, California who regularly
8 engages with Barack Obama, Dianne Feinstein, Nancy Pelosi, et al and their staff and political
9 financiers and receives billions of dollars of profits from government ‘favored nations contracts.

10 Zuckerberg was, at all times material to this Complaint, Facebook’s co-founder, Chief Executive
11 Officer, and a member of Facebook’s Board of Directors. Zuckerberg maintains his principal place
12 of business at Facebook’s headquarters at 1 Hacker Way, Menlo Park, California, 94025.

13 Since 2012, Zuckerberg has served as Chairman of Facebook’s Board and controls approximately
14 60% of the voting shares. At all times material to this Complaint, acting alone or in concert with
15 others, Zuckerberg was responsible for Facebook’s day-to-day operations, including the product
16 strategy of Facebook, and formulated, directed, controlled, had the authority to control, participated
17 in, or with knowledge, approved of the acts or practices of Facebook, including the acts and
18 practices set forth in this Complaint. Zuckerberg engages in the business of supplying social
19 networking services through the operation of his business, Facebook, which includes the product
20 Facebook and maintains a website, www.facebook.com, and accompanying mobile applications, to
21 consumers in D.C. Zuckerberg has traveled to Washington, D.C. on numerous occasions for matters
22 related to the District’s allegations, including to testify on Facebook’s activities to various agencies
23 and Congress.
24
25
26
27
28

Facebook’s Collection of Consumer Data for political Manipulation

The Facebook website allows consumers to build a social network with other Facebook consumers and share information within that network. It is among the world’s most heavily trafficked websites and has over two billion active consumers around the globe.

Hundreds of thousands of D.C. residents are among Facebook’s consumers. Millions of Californians are Facebook Consumers.

To begin using the Facebook website, a consumer first creates a Facebook account. The consumer can then add other Facebook consumers as “friends” and by accumulating Facebook friends, the consumer builds a social network on the Facebook website.

As Facebook consumers grow their social networks and interact with friends on the Facebook website, their information and activity are digitally collected, recorded, and maintained by Facebook. Relevant here, this data can be divided into two broad categories: (i) data directly supplied by consumers, and (ii) data pertaining to consumers’ activity on and off the Facebook website.

First, consumers directly provide Facebook with personal information. To create a Facebook account, a consumer is required to supply Facebook with basic information such as their name, phone number, email address, birthday, and gender. A consumer then has the option to customize their “Facebook Profile” by supplying additional information to Facebook, such as their hometown, educational history, work experience, relationship status, political and religious views, and personal photographs. Facebook’s website is designed to encourage consumers to continue supplying information in the form of “Posts,” which are shared with that consumer’s 4

In this Complaint, the “Facebook website” refers to both (i) www.facebook.com, which is accessed through an Internet browser, and (ii) the Facebook mobile application, which is accessed through a

CASE NO.: 22-cv-1107-TSH

1 mobile device like a smartphone or tablet. Many of Facebook’s features and services available on
2 www.facebook.com are also available through the Facebook mobile application.

3 Posts include, but are not limited to, written statements, photographs and videos, links to websites,
4 and “Check Ins” to geographic locations such as restaurants and bars.

5 Second, Facebook tracks and maintains data pertaining to consumer activity on its website, on other
6 websites on the Internet, and even what they do offline. For example, Facebook records what
7 advertisements are displayed to each consumer, as well as whether the consumer clicked on the
8 advertisement. Facebook also tracks the date and time each consumer logs into their account, as
9 well as the IP address, device, and browser they used to log in. Facebook also operates a companion
10 mobile application called “Facebook Messenger,” which allows Facebook consumers to send and
11 receive messages and make phone and video calls. For users of Facebook Messenger, Facebook
12 maintains records of messages sent and received and the date and time of phone and video calls
13 made.
14

15 Another example of consumer activity data that Facebook collects is a consumer’s “Likes,” one of
16 Facebook’s signature innovations. It allows consumers to click on a
17 “thumbs-up” icon to Like a vast array of online content. Among other things, Facebook consumers
18 can Like “Posts” made by other Facebook consumers, “Pages” maintained by non-individual
19 entities, and content on external websites.
20

21 Facebook’s Like feature incentivizes increased activity on the Facebook website by allowing
22 consumers to reward one another for sharing information—the more Posts a consumer makes, the
23 more Likes they will receive. The Like also serves a broader function because over time, a
24 consumer’s allocation of Likes reveals information about them—the friends they interact with most,
25 the brands that catch their eye, and the issues with which they identify.
26

27 Facebook records and maintains each and every one of its consumers’ Likes.
28

1 Facebook generates much of its revenue by selling advertising space. Facebook relies on its
2 collection of consumer data—and the personal information and preferences derived from each
3 individual’s data—to sell targeted advertising space to marketers. Facebook’s business model
4 primarily relies on using consumer data to provide advertisers the ability to run targeted ads to
5 particular individuals and demographics. In other words, although Facebook supplies its social
6 networking services free of direct monetary charge to consumers, in exchange, consumers provide
7 Facebook with their personal data, which Facebook monetizes through the sale of targeted
8 advertising.

9 **The Facebook Platform and Third-Party Facebook Applications**

11 In 2007, Facebook launched the Facebook “Platform,” an extensive software environment where
12 third-party developers can build applications that interact with the Facebook website. The Facebook
13 Platform includes various services and tools designed to assist third-party developers to create such
14 applications.

15 Millions of third-party applications have been developed using the Facebook Platform and made
16 available to Facebook consumers. Some applications are social, such as those that allow consumers
17 to play games against other consumers within their social networks. Others are functional, allowing
18 consumers to integrate information from their calendar and email accounts with their Facebook
19 account.

20 The Facebook Platform facilitates integration between the Facebook website and third-party
21 applications. For example, a third-party developer can allow Facebook consumers to access their
22 application with a service available on the Facebook Platform called “Facebook Login.” Facebook
23 Login allows a Facebook consumer to access an application directly by using 10

CASE NO.: 22-cv-1107-TSH

1 their Facebook account and login credentials (username and password). The Facebook Platform also
2 harmonizes third-party applications' look and feel with the Facebook website.

3 The Facebook Platform also includes an application program interface ("API").

4 An API specifies how software components interact. In practical terms, Facebook's website is built
5 upon proprietary source code. The API refers to the code that Facebook makes available to third-
6 party developers, which enables those developers to build applications for the Facebook website.

7 Facebook's API allows for a third-party application to interact with the Facebook website and
8 governs the extent to which it can access Facebook's vast collection of consumer data.
9

10 34.

11 In sum, the Facebook Platform was designed to allow for the development of third-party
12 applications that would seamlessly engage with Facebook consumers while at the same time
13 allowing those applications access to Facebook's vast collection of consumer data.

14 **The Cambridge Analytica Data Harvest**

15 The Harvest of 87 Million Facebook Consumers' Data

16
17 In November 2013, Aleksandr Kogan, a researcher affiliated with Cambridge University, and his
18 company, Global Science Research (GSR), launched a third-party application on the Facebook
19 Platform that identified itself as a personality study for research purposes. The application was
20 called "thisisyourdigitallife" (the "App") and ran on the Facebook Platform for over two years. The
21 App appealed to Facebook consumers as a personality quiz and offered to generate a personality
22 profile for consumers in exchange for downloading the App and granting access to some of the
23 consumer's Facebook data.

24
25 The App was presented to Facebook as a research tool to study psychological traits. At the time of
26 the App's launch, third-party applications could be launched on the 11

CASE NO.: 22-cv-1107-TSH

1 Facebook Platform without affirmative review or approval by Facebook. Accordingly, Facebook
2 did not review the App before it was allowed on the Facebook Platform, nor did it verify its claim
3 that the information it collected was for academic purposes.

4 At the time of the App's launch, Facebook permitted applications to request permission to access a
5 Facebook consumer's personal data. Prior to installation, a Facebook consumer installing the App
6 (an "App User") was shown a screen that stated that the App would download some of the App
7 User's own Facebook data, including their name, gender, birthdate, Likes, and a list of Facebook
8 friends.
9

10 To complete the installation, an App User clicked a Facebook Login icon on the information screen.
11 The App was then installed through the Facebook Login service, using the App User's Facebook
12 login credentials.

13 Upon installation, the App harvested the personal information of the App User from Facebook's
14 collection of user data, including at least the App User's name, gender, birthday, Likes, and list of
15 Facebook friends.
16

17 In addition, the App also accessed data of the App User's Facebook friends that the friend had
18 shared with the App User. This data included at least the Facebook friend's name, gender, birthdate,
19 current city, and Likes. The vast majority of these Facebook friends never installed the App, never
20 affirmatively consented to supplying the App with their data, and never knew the App had collected
21 their data.

22 In early 2014, Facebook introduced changes to the Facebook Platform that (i) limited the data that
23 applications could access, including data regarding the installing user's friends, and (ii) instituted a
24 review and approval process (called an "App Review") for applications that sought to access data
25 beyond what the updated Facebook Platform would allow.
26
27
28

CASE NO.: 22-cv-1107-TSH

1 In May 2014, Kogan applied to App Review to request access to consumer data beyond what the
2 updated Facebook Platform would allow. In only a matter of days, Facebook rejected Kogan's
3 application on the basis that he was seeking information beyond the App's stated research purposes.
4 Nevertheless, the App was not audited nor further investigated.

5 During the time that the App ran on the Facebook Platform, approximately 290,000 Facebook
6 consumers in the United States installed the App, including 852 consumers in D.C. Because the
7 App was improperly allowed to harvest the personal data of App Users as well as App Users'
8 Facebook friends, approximately 87 million Facebook consumers had their information collected by
9 the App, with more than 70 million in the United States—including over 340,000 District residents.
10

11
12 **The Sale and Misuse of Consumer Data by Political Parties and Government Officials For**
13 **Their Political Campaigns**

14 In 2014, at a time when the App was fully operational on the Facebook Platform and harvesting
15 consumer data, Kogan entered into an agreement with Cambridge Analytica for the sale of data
16 collected by the App. Cambridge Analytica was a political consulting firm based in London,
17 England that provided consulting services to candidates running for political office in the United
18 States and abroad.

19
20 Kogan provided Cambridge Analytica with the personal data of the approximately 87 million
21 Facebook consumers whose data was harvested, which included almost half of all D.C. residents. In
22 exchange, Cambridge Analytica paid Kogan over \$800,000.

23
24 Cambridge Analytica used the data it acquired from Kogan to, among other things, target digital
25 political advertising during the 2016 United States Presidential Election (the
26 "2016 Election"). Cambridge Analytica received millions of dollars from the Ted Cruz 13
27
28

CASE NO.: 22-cv-1107-TSH

1 presidential nomination campaign and later the Donald Trump presidential campaigns to provide
2 digital advertising services during the 2016 Election.

3 At relevant times, Facebook had employees embedded within multiple presidential candidate
4 campaigns who worked alongside employees from Cambridge Analytica.

5 Facebook knew, or should have known, that these presidential candidate campaigns and Cambridge
6 Analytica were using the Facebook consumer data harvested by Kogan throughout the 2016
7 Election.

8
9 **Facebook's Lack of Oversight and Enforcement of Its Own Policies *In Order To Help Corrupt***
10 ***Government Officials***

11 By no later than December 11, 2015, Facebook knew that Kogan had sold Facebook consumer data
12 to Cambridge Analytica. At that time, Facebook also knew that the collection and sale of consumer
13 data violated its Platform Policy.

14 Facebook's Platform Policy, which governed its relationship with third-party application developers
15 throughout the App's operation on the Facebook Platform, expressly prohibited the transfer and sale
16 of consumer data accessed from Facebook. However, Facebook failed to exert meaningful review or
17 compliance mechanisms to enforce its Platform Policy.

18 Indeed, the App itself contained terms that directly contradicted the Platform Policy, expressly
19 stating that collected data could be used for commercial purposes. Nevertheless, Facebook did not
20 take any action against the App and instead permitted it to harvest and sell Facebook consumers'
21 data without oversight for several years.

22 The Platform Policy also permitted Facebook to audit any applications on the Facebook Platform
23 and to take other enforcement measures if it suspected that an application was violating the Platform
24 Policy. In addition, the Platform Policy expressly provided several methods by which Facebook
25
26
27
28

CASE NO.: 22-cv-1107-TSH

1 could enforce non-compliance with the Platform Policy. These audit provisions were largely
2 unenforced.

3 In late December 2015, Facebook terminated the App's access to the Facebook Platform.

4 Nevertheless, Facebook did not ban, suspend, or limit the privileges of Kogan, Cambridge

5 Analytica, or any of their affiliates, with respect to their access to the Facebook website or the

6 Facebook Platform. Nor did Facebook conduct an audit of Kogan, Cambridge Analytica, or any of
7 their affiliates, or take any other enforcement or remedial action to determine whether the Facebook
8 consumer data that was harvested by the App had been accounted for, deleted, and protected from

9 further use and sharing.
10

11 Instead, Facebook simply requested that Kogan and Cambridge Analytica delete all data that they

12 received through the Facebook Platform and accepted their word that they had done so. Facebook

13 did not take any additional steps to determine whether the harvested data was, in fact, accounted for

14 and destroyed. And in fact, the data was not destroyed. It continued to be held and used by

15 Cambridge Analytica through the 2016 Election and beyond. Facebook knew, or should have

16 known, this fact from, among other sources, its employees embedded in presidential candidate

17 campaigns during the 2016 Election who worked alongside Cambridge Analytica employees.

18 Facebook eventually required written certifications promising that the harvested data was accounted

19 for and destroyed, but Facebook did not receive a certification from Kogan until June 2016 and did

20 not receive a certification from Cambridge Analytica until April 2017.
21

22 Facebook further kept this data harvesting a secret from its users for years, waiting until April 2018

23 to finally disclose to its consumers that their personal information may have been harvested and

24 sold to Cambridge Analytica.
25

26 Had Facebook and Zuckerberg disclosed in 2015 or 2016 the sale of Facebook consumer data to

27 Cambridge Analytica, they would have provided consumers with timely 15
28

1
2 material information about their use of the Facebook website. A disclosure that Facebook
3 consumers' data had been sold to a political consulting firm and was being used to target political
4 advertising for the 2016 Election could have influenced Facebook consumers, including those in
5 D.C. to, among other things, share less information on the Facebook website or deactivate their
6 Facebook accounts. Rather than make such meaningful disclosures, Facebook and Zuckerberg
7 instead profited from Kogan's and Cambridge Analytica's misuse of this stolen consumer data by
8 selling millions of dollars of advertising space to Cambridge Analytica and presidential candidate
9 campaigns during the 2016 Election.
10
11 Facebook knew of other third-party applications that similarly violated its Platform Policy through
12 selling or improperly using consumer data. Facebook also failed to take reasonable measures to
13 enforce its Platform Policy in connection with other third-party applications and failed to disclose to
14 users when their data was sold or otherwise used in a manner inconsistent with Facebook's policies.

15 **Facebook's Misleading Statements and Practices Regarding Third-Party Application Access**
16 **to Consumer Data**

17
18 Facebook's failure to disclose third-party applications' access to consumer data on its platform was
19 compounded by the fact that the limited disclosures Facebook did make were ambiguous,
20 misleading, and deceptive. These disclosures primarily are contained in two lengthy documents, a
21 Terms of Service and Data Policy, that consumers must agree to in order to create a Facebook
22 account. These documents together set out the general terms of use for the Facebook website and
23 contain some statements regarding how third-party applications could access a consumer's data.
24 However, as shown by Facebook's actions (and inactions) in connection with third parties,
25 including the App and Cambridge Analytica, the representations made in these documents were
26 misleading and deceptive. _
27
28

CASE NO.: 22-cv-1107-TSH

1 For the duration of the App's launch and operation on the Facebook Platform, Facebook's Terms of
2 Service represented that Facebook required applications to respect a Facebook consumer's privacy.
3 This representation, taken with Facebook's public statements that it would protect consumers'
4 private information and its representations in the Platform Policy that it had the ability to audit
5 applications and take enforcement measures against applications, gave consumers the impression
6 that Facebook had implemented and maintained reasonable oversight and safeguards to protect
7 consumers' privacy.

8
9 These representations were misleading and deceptive, as demonstrated by Facebook's lack of
10 oversight and enforcement relating to third parties, such as the App. For example, Facebook failed
11 to conduct meaningful oversight or enforcement of the App at several relevant times when it knew,
12 or should have known, that the App was operating in violation of Facebook's policies: (i) when the
13 App was first launched on the Facebook Platform; (ii) after Facebook became aware, through its
14 receipt and rejection of Kogan's application through App Review, that the App was seeking
15 consumer data to be used beyond the App's stated research purpose; and (iii) after it learned that
16 data collected by the App had been sold to Cambridge Analytica.

17
18 In addition, Facebook's Data Policy also contained misrepresentations about third-party
19 applications' access to Facebook consumer data. From at least November 15, 2013 to at least
20 January 30, 2015, the Data Policy provided that if an application asks permission from someone
21 else to access your information, the application will be allowed to use that information only in
22 connection with the person that gave the permission, and no one else. This representation was
23 deceptive and misleading as demonstrated by Kogan's use of the App to harvest consumer data, and
24 then sell it to Cambridge Analytica. Facebook failed to implement and maintain 17
25
26
27
28

CASE NO.: 22-cv-1107-TSH

1 Reasonable oversight of applications operating on the Facebook Platform to safeguard consumers’
2 private data, and it knew or should have known that it did not have measures in place to control how
3 applications used and/or shared data.

4 Facebook also misled its consumers generally about third-party applications’
5 access to their data. Facebook publicly represented that consumers controlled how their data is
6 shared on the Facebook website. But as shown by the App, third-party applications that a Facebook
7 consumer had never downloaded could still access their information through a Facebook friend who
8 downloaded the App. The Facebook Platform thus afforded third parties an end-run to access
9 consumer data, which third-party applications exploited. This was a material fact that Facebook
10 failed to disclose, or failed to adequately disclose, to its consumers. _
11

12
13 Adding to the potential customer confusion is the fact that consumers could not restrict third-party
14 application access to their data through Facebook’s Privacy Settings, even though that is where a
15 consumer would expect to have the ability to control how their data is shared. Instead, Facebook
16 allocated privacy settings related to applications to a separate location under a separate Application
17 Settings tab.
18

19 Through Privacy Settings, a consumer controls how their Facebook information is shared with other
20 Facebook consumers. For example, a consumer can control what kinds of other Facebook users can
21 view their account information. This can be manipulated to allow for sharing to all Facebook
22 consumers (most expansive), only Facebook friends (the less expansive default), and a customized
23 list of Facebook friends (the least expansive).
24

25 By contrast, through Application Settings, a consumer controls how their Facebook information is
26 shared with third-party applications. There is a high potential for consumer confusion here. For
27 example, from at least November 2013 through at least April 18
28

1
2 2014, even if a consumer restricted access to their information to only Facebook friends through
3 their Privacy Settings, the information could still be accessible by any application that the
4 consumer's friends downloaded.

5 In sum, Facebook's representations regarding consumer privacy in connection with applications
6 were misleading and deceptive. Moreover, Facebook's lack of adequate disclosures and multi-tiered
7 privacy options added to consumer confusion regarding how consumer information was shared with
8 applications.
9

10 Facebook's representations to consumers that it will protect the privacy of consumers' personal
11 information, when, in fact, it did not implement or maintain reasonable privacy safeguards and
12 failed to take reasonable measures in response to the harvesting and use of data by Cambridge
13 Analytica, are misrepresentations of material facts that tend to mislead consumers.

14 Facebook's representations to consumers that it requires applications and third-party developers to
15 respect the privacy of consumers' personal information, when, in fact, it did not implement or
16 maintain reasonable oversight of third-party applications (such as conduct appropriate audits of
17 applications), are misrepresentations of material facts that tend to mislead consumers.
18

19 Facebook's representations to consumers that consumers' agreements with third-party applications
20 will control how those applications use consumer data, when, in fact, applications were able to
21 collect and use consumer data without regard to those agreements, are misrepresentations of
22 material facts that tend to mislead consumers.
23

24 Facebook's failure to inform consumers, or to adequately inform consumers, that their personal
25 information may be shared with third-party applications without their knowledge or affirmative
26 consent, is a material fact, the omission of which tended to mislead consumers.
27
28

CASE NO.: 22-cv-1107-TSH

Facebook’s failure to tell consumers for over two years that their personal information was improperly harvested and sold by Kogan to Cambridge Analytica in violation of Facebook’s policies is a material fact, the omission of which tended to mislead consumers.

Facebook’s failure to explain to consumers whether and how they could control how information is shared with third-party applications and how to change privacy settings with respect to applications, and its representations that consumers can control how their information is shared, constitute ambiguities as to material facts that have the tendency to mislead consumers.

Mark Zuckerberg’s Control Over the Facebook Platform

Zuckerberg’s role and responsibility at Facebook

Zuckerberg is Facebook’s co-founder, CEO, and Chairman, and is inseparable from the company he founded. He continues to manage the company’s day-to-day operations—at an exacting level of detail—including directing, participating in, and guiding the Facebook Platform.

He maintains an unparalleled level of control over the operations of Facebook as it has grown into the largest social media company in the world. In fact, throughout Facebook’s inception and explosive growth, Zuckerberg has retained control of the company. Zuckerberg currently controls almost 60% of Facebook’s voting shares and has the power to appoint a majority of the company’s board members.

Zuckerberg is not just a figurehead at Facebook; he is personally involved in nearly every major decision the company makes, and his level of influence is no secret. Dave 20

Arnold, a Facebook spokesman, recently touted Zuckerberg’s “active” leadership in the *New York Times* stating, “Mark has taken an active role in the leadership of Facebook from its founding

CASE NO.: 22-cv-1107-TSH

1 through to today . . . We're fortunate to have such engaged leaders, including Mark, Sheryl and the
2 entire leadership team.”

3 Zuckerberg not only manages the company, but he also serves as the driving force behind its
4 products. Early versions of the Facebook Platform—which promoted the “concept of openness and
5 transparency as the high level ideal”—arose from Zuckerberg’s vision.⁶ According to Zuckerberg,
6 Facebook “actually shifted a bit more of a focus not just on directly making it so people can use
7 Facebook and share and be open on Facebook, but instead on making it so that the *systems*
8 *themselves have open properties.*”
9

10 Zuckerberg has even gone as far as claiming that privacy is no longer a “social norm” because
11 “[p]eople have really gotten comfortable not only sharing more information and different kinds, but
12 more openly and with more people[.]”⁸

13 Zuckerberg’s vision of “open properties” directly led to developing the API tool called “Open
14 Graph” that Facebook launched in April 2010 as Graph API version 1.0. Open Graph allowed
15 consumers to personalize their user experience and “have instantly social connection”
16

17 IE:

18 Mike Isaac, Sheera Frenkel, and Cecilia Kang, *Now More Than Ever, Facebook Is a*

19 *‘Mark Zuckerberg Production’*, NEW YORK TIMES (May 16, 2020),

20 <https://www.nytimes.com/2020/05/16/technology/zuckerberg-facebook-coronavirus.html>.

21 Fred Vogelstein, *The Wired Interview: Facebook’s Mark Zuckerberg*, WIRED (June 29, 2009),

22 <https://www.wired.com/2009/06/mark-zuckerberg-speaks/>.

23 *Id.* (emphasis added).

24 *Marshall Kirkpatrick, Facebook’s Zuckerberg Says The Age of Privacy Is Over*, NEW

25 YORK TIMES (Jan. 10, 2020),
26
27
28

CASE NO.: 22-cv-1107-TSH

1 <https://archive.nytimes.com/www.nytimes.com/external/readwriteweb/2010/01/10/10readwriteweb-facebooks-zuckerberg-says-the-age-of-privac-82963.html>.

2
3 But to create these experiences, Facebook made information such as a person's likes, dislikes, and
4 interests instantly viewable to the person's Facebook friends—and gave developers access to that
5 personal data—including access to the data of a user's Facebook friends, with little to no oversight.

6 On April 21, 2010, Zuckerberg publicly unveiled Graph API version 1.0 at Facebook's annual F8
7 App Developer conference, saying: "We are building a web where the default is social." 10 For
8 Zuckerberg, "[t]he thing [he] really care[d] about is the mission, making the world open." 11

9
10 Shortly thereafter however, Facebook faced criticism over the growing concern from Facebook
11 users and lawmakers that Graph API version 1.0 greatly expanded the scope of publicly available
12 data to applications and developers by automatically allowing access to a user's current city,
13 hometown, education, work, likes, interests, and friends list without user consent. 12

14 Zuckerberg responded by posting a public apology in the *Washington Post* acknowledging that
15 "[s]ometimes we move too fast—and after listening to recent concerns,
16 IE:

17
18 Erick Schonfeld, *Zuckerberg: "We are Building a Web Where the Default is Social"*,
19 TECHCRUNCH (Apr. 21, 2010), [https://techcrunch.com/2010/04/21/zuckerbergs-buildin-web-](https://techcrunch.com/2010/04/21/zuckerbergs-buildin-web-default-social/)
20 [default-social/](https://techcrunch.com/2010/04/21/zuckerbergs-buildin-web-default-social/).

21 Ryan Singel, *Mark Zuckerberg: I Donated to Open Source, Facebook Competitor*, WIRED (May
22 20, 2010), <https://www.wired.com/2010/05/zuckerberg-interview/>.

23
24 Jason Kincaid, *Senators Call Out Facebook On 'Instant Personalization', Other Privacy Issues*,
25 TECHCRUNCH (Apr. 27, 2010), [https://techcrunch.com/2010/04/27/senators-call-out-facebook-](https://techcrunch.com/2010/04/27/senators-call-out-facebook-on-instant-personalization-other-privacy-issues/?_ga=2.192578537.216944569.1650296804-940477689.1650296804)
26 [on-instant-personalization-other-privacy-](https://techcrunch.com/2010/04/27/senators-call-out-facebook-on-instant-personalization-other-privacy-issues/?_ga=2.192578537.216944569.1650296804-940477689.1650296804)
27 [issues/?_ga=2.192578537.216944569.1650296804-940477689.1650296804](https://techcrunch.com/2010/04/27/senators-call-out-facebook-on-instant-personalization-other-privacy-issues/?_ga=2.192578537.216944569.1650296804-940477689.1650296804).

1
2 The biggest message we have heard recently is that people want easier control over their
3 information. Simply put, many of you thought our controls were too complex.

4 Our intention was to give you lots of granular controls; but that may not be what many of you
5 wanted. We just missed the mark.

6 We have heard the feedback. There needs to be a simpler way to control your information. In the
7 coming weeks, we will add privacy controls that are much simpler to use. We will also give you an
8 easy way to turn off all third-party services.

9
10 Within Facebook, Zuckerberg directly oversaw the product development and engineering work that
11 was exposing consumer data to abuse: Zuckerberg is in charge of the Facebook Platform and is able
12 to overrule any decisions made by the company. But Zuckerberg's involvement includes not only
13 deciding just *how* open the Facebook Platform should be and what categories of user data should be
14 shared with developers—he is also making day-to-day decisions about minute details of the
15 Platform's operations, including specific policy changes and enforcement decisions.

16
17 And contrary to his public statements, Zuckerberg was intent on finding a way of leveraging
18 Platform changes to amass more data—and accordingly more money—for Facebook.

19 In November 2012, Zuckerberg unveiled his plan for Facebook's data-sharing business model—
20 which included giving apps and developers who spent money on Facebook or shared data back to
21 Facebook—access to *even more* consumer data.

22 IE:

23 Mark Zuckerberg, *From Facebook, answering privacy concerns with new settings*, WASHINGTON
24 POST (May 24, 2010),

25 <https://www.washingtonpost.com/wp-dyn/content/article/2010/05/23/AR2010052303828.html>.
26
27
28

CASE NO.: 22-cv-1107-TSH

1 n a November 19, 2012, email to senior-level Facebook executives entitled “Platform Model
2 Thoughts,” Zuckerberg discussed the value of “pulling non-app friends out of friends.get”—in other
3 words making friends’ data available only through private APIs, which would further obfuscate a
4 developers’ ability to access data from Facebook consumers:

5 After thinking about platform business for a long time, I wanted to send out a note explaining where
6 I’m leaning on this. This isn’t final and we’ll have a chance to discuss this in person before we
7 decide this for sure, but since this is complex, I wanted to write out my thoughts. This is long, but
8 hopefully helpful. The quick summary is that I think we should go with full reciprocity and access
9 to app friends for no charge. Full reciprocity means that apps are required to give any user who
10 connects to FB a prominent option to share all of their social content within that service [...] back to
11 Facebook. [...]

12 [W]e’re trying to enable people to share everything they want, and to do it on Facebook.

13 Sometimes the best way to enable people to share something is to have a developer build a special
14 purpose app or network for that type of content and to make that app social by having Facebook
15 plug into it. However, that may be good for the world but it’s not good for us unless people also
16 share back to Facebook and that content increases the value of our network. So ultimately, I think
17 the purpose of platform—even the read side—is to increase sharing back into Facebook.

18 [...]

19 It seems like we need some way to fast app switch to the FB app to show a dialog on our side that
20 lets you select which of your friends you want to invite to an app. We need to make sure this
21 experience actually is possible to build and make as good as we want, especially on iOS where
22 we’re more constrained. We also need to figure out how we’re going to charge for it. I want to make
23 sure this is explicitly tied to pulling non-app friends out of friends.get.
24
25
26
27
28

1 [...] 2

3 What I'm assuming we'll do here is have a few basic thresholds of API usage and once you pass a
4 threshold you either need to pay us some fixed amount to get to the next threshold or you get rate
5 limited at the lower threshold.

6 [...] 7

8 Overall, I feel good about this direction. The purpose of platform is to tie the universe of all the
9 social apps together so we can enable a lot more sharing and still remain the central social hub. I
10 think this finds the right balance between ubiquity, reciprocity and profit.

11 Zuckerberg's data-sharing business model underscores just how Facebook was able to get
12 developers to use the Platform and why apps were able to amass so much Facebook consumer data:
13 by leveraging access to friend data, Facebook's "most valuable data."

14 To carry out his business vision for Facebook, Zuckerberg oversaw changes to the Platform
15 policies, including at the granular level of providing specific direction and assigning employees to
16 the task. For example, in a November 19, 2012 email, Zuckerberg assigned specific employees,
17 including former Harvard classmate Sam Lessin and longtime Facebook employee Javier Olivan,
18 Head of International Growth, to the task of putting together a "real framework and process" for
19 enforcement actions, giving them guidelines to create a process that is
20 "minimally intrusive/annoying" and "as simple as we can get away with."

21 Zuckerberg also provided direct input on Facebook's internal policies relating to data sharing on the
22 Platform, and was so involved that he personally reviewed certain applications' use of data. This
23 was especially true for developers who Facebook deemed "competitors" and were therefore
24 restricted from accessing certain categories of data, such as friend data, on the Platform. While
25 making Facebook data generally available to developers was in Facebook's interests, that decision
26 cut the other way when it came to competitors.
27
28

1 IE:

2 Email from Mark Zuckerberg to Sam Lessin (Nov. 19, 2012, 10:39 a.m.), available at

3 [https://dataviz.nbcnews.com/projects/20191104-facebook-leaked-documents/assets/facebook-](https://dataviz.nbcnews.com/projects/20191104-facebook-leaked-documents/assets/facebook-sealed-exhibits.pdf)
4 [sealed-exhibits.pdf](https://dataviz.nbcnews.com/projects/20191104-facebook-leaked-documents/assets/facebook-sealed-exhibits.pdf).

5 Email from Douglas Purdy to Constantin Koumouzelis, Marie Hagman, Zhen Fang, Eddie O’Neil,
6 and George Lee (Apr. 10, 2013, 8:25 p.m.), available at

7 [https://dataviz.nbcnews.com/projects/20191104-facebook-leaked-documents/assets/facebook-](https://dataviz.nbcnews.com/projects/20191104-facebook-leaked-documents/assets/facebook-sealed-exhibits.pdf)
8 [sealed-exhibits.pdf](https://dataviz.nbcnews.com/projects/20191104-facebook-leaked-documents/assets/facebook-sealed-exhibits.pdf).

9
10 ***Any changes on the Platform relating to these competitors would be escalated to Zuckerberg for***
11 ***approval and only permitted after his sign-off.***

12 For example, in an April 2013 email, Doug Purdy, Facebook’s Director of Product Management,
13 discussed an internal plan to implement certain API restrictions stating,

14 “We maintain a small list of strategic competitors that Mark personally reviewed. Apps produced by
15 the companies on this list are subject to a number of restrictions outlined below. Any usage beyond
16 that specified is not permitted without Mark level sign-off.”

17
18 Zuckerberg also instructed top-level executives to enforce Facebook’s “policies against competitors
19 much more strongly.”²⁰ In January 2013, Zuckerberg confirmed a new Facebook policy blocking
20 competitors WeChat, Kakao, Line, and Google+ products from spending on ads or accessing friend
21 data on the Platform, noting “[t]hose companies are trying to build social networks and replace us.

22 The revenue is immaterial to us compared to any risk.”

23 Similarly, in a January 24, 2013 email, Zuckerberg gave the green light to Justin Osofsky,

24 Facebook’s former Vice President of Global Operations, to “shut down” Vine, a popular video-

25 sharing app’s access to the “friends API”—that app was owned by Facebook’s competitor Twitter,

26 Inc.
27
28

1
2 Email from Mark Zuckerberg to Sam Lessin (Nov. 19, 2012, 10:39 a.m.), available at

3 [https://dataviz.nbcnews.com/projects/20191104-facebook-leaked-documents/assets/facebook-](https://dataviz.nbcnews.com/projects/20191104-facebook-leaked-documents/assets/facebook-sealed-exhibits.pdf)
4 [sealed-exhibits.pdf](https://dataviz.nbcnews.com/projects/20191104-facebook-leaked-documents/assets/facebook-sealed-exhibits.pdf).

5
6 Email from Mark Zuckerberg to Javier Olivan, Sheryl Sandberg, Dan Rose, Mike Vernal, Justin
7 Osofsky, Elliot Schrage, Sam Lessin, et. al. (Jan. 10, 2013, 1:28 a.m.), available at

8 [https://dataviz.nbcnews.com/projects/20191104-facebook-leaked-documents/assets/facebook-](https://dataviz.nbcnews.com/projects/20191104-facebook-leaked-documents/assets/facebook-sealed-exhibits.pdf)
9 [sealed-exhibits.pdf](https://dataviz.nbcnews.com/projects/20191104-facebook-leaked-documents/assets/facebook-sealed-exhibits.pdf).

10
11
12 Email from Dan Rose to Mike Vernal, Justin Osofsky, Mark Zuckerberg, Kevin Systrom, Douglas
13 Purdy and Dan Rose (Jan. 24, 2013, 12:21 p.m.), available at

14 [https://dataviz.nbcnews.com/projects/20191104-facebook-leaked-documents/assets/facebook-](https://dataviz.nbcnews.com/projects/20191104-facebook-leaked-documents/assets/facebook-sealed-exhibits.pdf)
15 [sealed-exhibits.pdf](https://dataviz.nbcnews.com/projects/20191104-facebook-leaked-documents/assets/facebook-sealed-exhibits.pdf).

16
17 Zuckerberg was aware of the risks posed by an “Open” Platform but failed to act because he was
18 told to control elections and he could not do so as well as he could if he followed the rules.

19 Zuckerberg was personally aware of the risks that sharing consumer data with apps posed, but
20 actively disregarded those risks because sharing data was otherwise beneficial and lucrative to
21 Facebook’s business model and Platform growth.

22 Even as early as 2012, Zuckerberg was aware of potential harms that might result from sharing
23 consumer data. In an October 27, 2012, email concerning apps leaking personal data, Zuckerberg
24 stated,

25
26 I’m getting more on board with locking down some parts of platform, including friends’
27
28

CASE NO.: 22-cv-1107-TSH

1 data and potentially email addresses for mobile apps. I'm generally skeptical that there is as much
2 data leak strategic risk as you think. *I agree there is clear risk on the advertiser side*, but I haven't
3 figured out how that connects to the rest of the platform. *I think we leak info to developers*, but I
4 just can't think of any instances where that data has leaked from developer to developer and caused
5 a real issue for us.

6 Despite being aware of risks on the Platform, Zuckerberg failed to take the necessary steps to
7 protect consumer data—including the personal data of hundreds of thousands of District consumers.

8 Just months before the Cambridge Analytica data harvest became public, Zuckerberg admitted that
9 his “personal challenge for 2018” was to fix abuse on the platform:
10

11 “we currently make too many errors enforcing our policies and preventing misuse of our tools.”

12 When details about Cambridge Analytica became public in March 2018, Zuckerberg publicly
13 IE:

14 Email from Mark Zuckerberg (Oct. 27, 2012, 6:06 a.m.), available at

15 [https://dataviz.nbcnews.com/projects/20191104-facebook-leaked-documents/assets/facebook-](https://dataviz.nbcnews.com/projects/20191104-facebook-leaked-documents/assets/facebook-sealed-exhibits.pdf)
16 [sealed-exhibits.pdf](https://dataviz.nbcnews.com/projects/20191104-facebook-leaked-documents/assets/facebook-sealed-exhibits.pdf).

17
18
19 Mark Zuckerberg, FACEBOOK (Jan. 4, 2018),

20 <https://www.facebook.com/zuck/posts/10104380170714571> (last visited May 20, 2022).

21
22 acknowledged the incident as a “breach of trust between Facebook and the people who share their
23 data with us and expect us to protect it.”

24
25 Zuckerberg's shift in tone and acknowledgment of Cambridge Analytica shows Facebook knew it
26 could no longer hide behind its lax enforcement actions in the past. At Zuckerberg's direction,

CASE NO.: 22-cv-1107-TSH

Facebook shifted to promising future improvements to the security of the Platform, thereby hoping to obscure the company's past harms and failures to adequately protect users' privacy.

For example, despite Facebook's ability to audit apps well before Cambridge Analytica became public in 2018, Zuckerberg vowed only after the breach became public to "conduct a full audit of any app with suspicious activity" and promised to "ban any developer from our platform that does not agree to a thorough audit."²⁶ Zuckerberg also promised additional restrictions on developers' access to user data and additional tools to help users more easily "revoke those apps' permissions to [user] data."

Zuckerberg has publicly taken personal responsibility for Facebook's failures leading up the Cambridge Analytica incident as well. In April 2018 at a Congressional hearing relating to data privacy, Zuckerberg himself testified, "I started Facebook, I run it, and I'm responsible for what happens here."²⁸ In another statement in April 2018 concerning data privacy

IE:

Mark Zuckerberg, FACEBOOK (Mar. 21, 2018),

<https://www.facebook.com/zuck/posts/10104712037900071> (last visited May 20, 2022).

Facebook CEO Mark Zuckerberg Hearing on Data Privacy and Protection, C-SPAN

(Apr. 10, 2018), <https://www.c-span.org/video/?443543-1/facebook-ceo-mark-zuckerberg-testifies-data-protection> (complete opening statement in Senate Hearing).

on the Platform, Zuckerberg stated, "We didn't take a broad enough view of what our responsibility is, and that was a huge mistake. *It was my mistake.*"

In sum, Zuckerberg is broadly responsible for his Platform "vision" which required implementing an open Platform and exposing consumers' personal data, was aware of the trade-off between the

CASE NO.: 22-cv-1107-TSH

1 security of users' data and Facebook's own profits that these choices posed, and was directly
2 responsible for Facebook's lax enforcement standards and actions.

3 As CEO, Zuckerberg had the authority to control and direct—and had knowledge of—Facebook's
4 deceptive trade practices and misrepresentations to District consumers.

5 As such, Zuckerberg participated in, directed, managed, or otherwise knew of, and had the authority
6 to control, Facebook's inconsistent actions regarding privacy, including deceptive trade practices,
7 misrepresentations, and ambiguities that violate the CPPA—namely: a.

8 Facebook's representations to consumers that Facebook would protect the privacy of consumers'
9 personal information, when, in fact, it did not implement or maintain reasonable privacy safeguards
10 and failed to take reasonable measures in response to the harvesting and use of data by Cambridge
11 Analytica;
12

13
14 Facebook's representations to consumers that it requires applications and third-party developers to
15 respect the privacy of consumers' personal information, when, in fact, it did not implement or
16 maintain reasonable oversight of third-party applications (such as conduct appropriate audits of
17 applications);
18

19 Facebook's representations to consumers that consumers' agreements with third-party applications
20 will control how those applications use consumer data, when, in fact, applications were able to
21 collect and use consumer data without regard to those agreements;
22

23 Facebook's failure to inform consumers, or to adequately inform consumers, that their personal
24 information may be shared with third-party
25
26
27
28

CASE NO.: 22-cv-1107-TSH

1 *Hard Questions: Q&A With Mark Zuckerberg on Protecting People's Information*, FACEBOOK
2 NEWSROOM (Apr. 4, 2018), [https://about.fb.com/news/2018/04/hard-questions-protecting-](https://about.fb.com/news/2018/04/hard-questions-protecting-peoples-information/)
3 [peoples-information/](https://about.fb.com/news/2018/04/hard-questions-protecting-peoples-information/) (emphasis added).

4 ... applications without their knowledge or affirmative consent; e.

5 Facebook's failure to tell consumers for over two years that their personal information was
6 improperly harvested and sold by Kogan to Cambridge Analytica in violation of Facebook's
7 policies; and

8
9 Facebook's failure to explain to consumers how to control how information is shared with third-
10 party applications and how to change privacy settings with respect to applications, and its
11 representations that consumers can control how their information is shared.

12
13 **Count I: Violations of the Consumer Protection Procedures Act**

14
15 The District incorporates by reference the foregoing allegations.

16
17 100. The CPPA is a remedial statute that is to be broadly construed. It establishes an enforceable
18 right to truthful information from merchants about consumer goods and services that are or would
19 be purchased, leased, or received in the District of Columbia.

20 101. The services that Facebook provides consumers are for personal, household, or family
21 purposes and, therefore, are consumer goods and services.

22 102. Facebook, in the ordinary course of business, supplies consumer goods and services and,
23 therefore, is a merchant under the CPPA.

24
25 103. Facebook users receive consumer goods and services from Facebook in the form of social
26 networking services and, therefore, are consumers under the CPPA.

CASE NO.: 22-cv-1107-TSH

104. The CPPA prohibits unfair and deceptive trade practices in connection with the offer, sale, and supply of consumer goods and services.

105. Facebook’s representations to consumers, both express and implied, that it will protect the privacy of consumers’ personal information, that it requires applications and third-party developers to respect the privacy of consumers’ personal information, and that consumers’

agreement with third-party applications will control how those applications use consumer data, 30

are misrepresentations concerning material facts that have a tendency to mislead consumers and are unfair and deceptive trade practices that violate the CPPA, D.C. Code § 28-3904(e).

106. Facebook’s failure to disclose, or failure to adequately disclose, to consumers that their personal information may be shared with third-party applications without their knowledge or affirmative consent, is a material fact, the omission of which tended to mislead consumers and are unfair and deceptive trade practices that violate the CPPA, D.C. Code § 28-3904(f).

107. Facebook’s failure to disclose, or failure to adequately disclose, to consumers that their personal information was improperly harvested and used by third-party applications and others in violation of Facebook’s policies, such as in the Kogan and Cambridge Analytica example, is a material fact, the omission of which tended to mislead consumers and are unfair and deceptive trade practices that violate the CPPA, D.C. Code § 28-3904(f).

108. Facebook’s failure to explain to consumers how to control how information is shared with third-party applications and how to change privacy settings with respect to applications, as well as its representations to consumers, both express and implied, that it will protect the privacy of consumers’ personal information, that it requires applications and third-party developers to respect the privacy of consumers’ personal information, and that consumers’

CASE NO.: 22-cv-1107-TSH

1 agreement with third-party applications will control how those applications use consumer data,
2 constitute ambiguities as to material facts that have the tendency to mislead consumers and are
3 unfair and deceptive trade practices that violate the CPPA, D.C. Code § 28-3904(f-1).

4 109. At all times relevant to this Complaint, Defendant Mark Zuckerberg (i) was aware or should
5 have been aware of Facebook's data-sharing policy terms; (ii) possessed and/or exercised the
6 authority to control the policies and practices of Facebook, Inc.; (iii) was responsible for creating
7 and implementing the deceptive policies and trade practices of 31
8

9
10 Facebook, Inc. that are described in this Complaint; (iv) participated in the deceptive trade practices
11 that are described in this Complaint; (v); directed, managed, or supervised, those employees at
12 Facebook, Inc. who participated in the deceptive trade practices described in this Complaint; and
13 (vi) knew or should have known of the deceptive trade practices that are described in this Complaint
14 and had the power to stop them, but did not. “
15

16 While much that is revealed in the above is disturbing regarding the rights of Plaintiff, it is
17 VERY disturbing for every citizen in the world. How could a company grow to become so vast, so
18 evil, so manipulative of industry, elections and information unless corrupt government officials,
19 THAT OWN FACEBOOK, GOOGLE, NETFLIX, TESLA, et al, were protecting and directing that
20 company? It is IMPOSSIBLE for Facebook to have grown so large and so corrupt without Mark
21 Zuckerberg exchanging compensation with government officials including those mentioned herein,
22 who he knows, personally. The recordings between Barack Obama, David Plouffe, Nancy Pelosi,
23 the Zuckerbergs and others reveal hard core conspiracy and is not a THEORY! The DC court
24 evidence reveals hard core conspiracy and is not a THEORY! The leaked public officials emails and
25 text messages reveal hard core conspiracy and is not a THEORY! Government officials used
26 FACEBOOK, GOOGLE, NETFLIX, TESLA, et al, WHICH: 1.) THEY OWN; 2.) GET MONEY
27
28

CASE NO.: 22-cv-1107-TSH

FROM; 3.) GET ELECTION MANIPULATION SERVICES FROM; 4.) THEY PARTY, DINE, HAVE SEX AND ORGANIZE WITH: AND ENGAGE IN HUNDREDS OF OTHER CONFLICTS OF INTEREST WITH!

In this, or another court trial, some Plaintiff is going to subpoena every bank and account record of FACEBOOK, GOOGLE, NETFLIX, TESLA, et al,. (FINCEN already has such records and could introduce them in lieu of a subpoena). Every wire transfer from ANY government account to FACEBOOK, GOOGLE, NETFLIX, TESLA, et al, will be scrutinized in detail, since 2000, and compared with what their competitors received during the same time frame. Wouldn't it be interesting if certain public officials, who are Mark's buddies, arranged to get contracts for Facebook, that nobody else got, while those officials were in office?

The bottom line is that there is now hard core forensic evidence on the books that proves that the government allowed its executives and officials to own, protect from regulation and operate illicit Silicon Valley operations that used their resources to harm Plaintiff, harm industry, harm society, harm elections and cause the deaths of children who were not immune to their Bullying-As-A-Service business models!

DATED this day of the filing of 2022

Respectfully submitted,

(SIGNED ELECTRONICALLY)

Name: SD Redmond

**Address: 210 S. Ellsworth Ave, #1275
San Mateo, CA 94401**

Phone Number: 510-868-2862

E-mail Address: justice@majestic111.com

Pro Se – A federal witness

EXHIBITS AND PROOFS ARE PROVIDED AS SEPARATE NUMBERED DOCUMENTS

Pg 36 of 18, ATTACKERS EXHIBIT FACEBOOK GOOGLE- 5.23.22 – NorCal 9th District -

CASE NO.: 22-cv-1107-TSH

(PAGES PAST THIS SENTENCE ARE INTENTIONALLY BLANK)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28